CASL COMPLIANCE TOOLKIT

A Guide to Preparing Your Business for Canada's Anti-Spam Legislation

excalibur INSURANCE GROUP

Provided by: Excalibur Insurance Group

56 Albert Street Box 191

Clinton, ON N0M 1L0

Tel: (519) 482-9357

The information contained in this toolkit is not intended to be used as legal advice. The reader should consult legal counsel regarding specific legal issues.
© 2014 Zywave Inc. All Rights Reserved.

Introduction

Canada's Anti-Spam Legislation (CASL) was created to protect Canadian citizens from unwanted electronic communication or computer program installation – collectively known as "spam." CASL applies to all businesses or individuals who send commercial electronic messages or install computer programs in Canada or for an entity operating in Canada. CASL will come into force in three parts:

- Rules that apply to sending commercial electronic messages – July 1, 2014
- Rules governing computer program installation – Jan. 15, 2015
- Private right of action – July 1, 2017

The repercussions for non-compliance with CASL are severe. Companies that send CEMs or install computer programs should examine how CASL will impact corporate business practices and enact procedures to ensure complete compliance. This toolkit provides 12 resources to help your company remain in compliance.

Table of Contents

Employer Resources

Sample CASL Compliance Plan 3
Legislative Brief: Canada's Anti-Spam Legislation (CASL) 4
Legislative Take Action – CASL Compliant Commercial Electronic Messages 7
Legislative Take Action – FAQ on CASL and CEMs 9
Legislative Take Action – CASL Computer Program Compliance 11
CEM Inventory Worksheet 13
Sample CASL Compliance Agreement 14
CASL – Sample CEM Compliance Policy 16

Employee Resources

Cyber Liability – Spam, Phishing and Spyware Defined 19
Playing it Safe: Surf the Internet Safely 21
Can I Send It? Flowchart 23
Surf Safe Poster 24

CASL Compliance Plan

A sample step-by-step approach to compliance with Canada's Anti-Spam Legislation

Timeline	Action	Supporting Materials
April 2014	Establish CASL Compliance committee. Select representatives from senior management, marketing, legal, information technology, human resources and risk management. Supply members with basic information about CASL.	Legislative Brief: Canada's Anti-Spam Legislation (CASL) Legislative Take Action – CASL Compliant Commercial Electronic Messages Legislative Take Action – FAQ on CASL and CEMs
	Complete the CEM Inventory. List all current contacts and note whether consent is express or implied or the recipient is exempt. List when consent expires. Update the CEM Inventory quarterly.	CEM Inventory Worksheet
May 2014	Solicit express consent from existing contacts.	
	Establish a mechanism for obtaining express consent from new contacts.	
	Update existing email templates to include unsubscribe mechanism and sender contact information.	
June 2014	Review third-party relationships and update contracts. Determine whether third party will be sending CEMs or installing computer programs or updates on your behalf.	Sample CASL Compliance Agreement
	Draft corporate CASL compliance policy.	CASL – CEM Compliance Policy
	Train staff on CASL Compliance policy, corporate procedure for sending CEMs and safe computer use.	Cyber Liability - Spam, Phishing and Spyware Defined Playing it Safe: Surf Safe Surf Safe Poster Can I Send It
	Consult with Excalibur Insurance Group to determine whether additional insurance is necessary.	
Prior to Jan. 1, 2015	If use of your company product requires that users install computer programs, you should develop consent mechanisms, disclosures and notices.	Legislative Take Action – CASL Computer Program Compliance

Legislative
Brief

Canada Anti-Spam Legislation (CASL)

Provided by Excalibur Insurance Group

Quick Facts

CASL places restrictions on the following forms of electronic commerce:

- Unsolicited or false and misleading CEMs
- Data transmission
- Computer program installation
- E-address and personal information collection

Any organization that uses commercial electronic messages, alters data transmissions or produces or installs computer programs should take note of the anti-spam legislation.

On Dec. 22, 2010, the Canadian House of Commons passed Bill C-28, Canada's Anti-Spam Legislation (CASL). The purpose of this law is, in part, to regulate unsolicited commercial electronic messages (CEMs), commonly referred to as "spam." Following a December 2013 Governor in Council order, most provisions of the law will come into force on **July 1, 2014**. Additional sections of the law related to the unsolicited installation of computer programs or software will come into force on Jan. 15, 2015, and the private right of action provisions will come into force on July 1, 2017.

Any organization that uses CEMs, alters data transmissions or produces or installs computer programs should take note of the law and examine the effect it may have on its business practices.

Prohibition on Sending CEMs

The anti-spam law places restrictions on the following forms of electronic commerce:

- Unsolicited or false and misleading CEMs;
- Data transmission;
- Computer program installation; and
- E-address and personal information collection.

Though the CASL has a wide scope, the most relevant requirements for the majority of businesses relate to sending CEMs. Sending CEMs to an e-address, without consent, is **prohibited** under the law. The law restricts all forms of CEMs sent via telecommunication, including, but not limited to:

- Email messages;
- Text and picture messages;
- Instant messages; and
- Messages sent through social networking sites.

In order to qualify as commercial, CEMs only need to encourage commercial conduct and do not need to have an underlying expectancy of profit.

Express Consent to Receive CEMs

In general, all organizations must obtain express consent to send a CEM to any recipient prior to sending the message. This means that recipients must "opt in" to receive CEMs. Consent may be obtained either orally or in writing. In order for consent to be valid, all

© 2013, 2014 Zywave, Inc. All rights reserved.

senders must include the following content in the request for consent:

- The purpose or purposes for the consent being sought;
- Identifying information of the sender and his or her business;
- A statement informing the recipient that he or she may withdraw consent at any time;
- The sender's mailing address and a phone number, email address or Web address; and
- A statement identifying the person asking for consent.

The burden of proving that consent has been obtained falls to the sender. In limited cases, organizations may avoid obtaining express consent if implied consent exists.

Implied Consent to Receive CEMs

In limited circumstances, CEM senders can avoid express consent requirements if the sender can establish that the recipient implicitly consented to receiving the CEM. Recipient consent is implied for a three-year transitional period if a pre-existing business relationship already exists between the sender and the recipient. Prior business relationships can be established in situations where:

- The recipient purchased or leased goods, land or services within the previous two years;
- The recipient agreed to a business or investment opportunity within the previous two years; or
- The recipient made an inquiry or application for business purposes within the previous six months.

Implied consent is also granted in certain non-business relationships, including situations where (i) the recipient provided qualifying donations or volunteer work; (ii) the CEM is provided in a conspicuous publication; or (iii) the message is directly related to the recipient's role in a business or profession. Even if a sender can establish implied consent, the sender must still provide the recipient with a mechanism to withdraw consent from receiving CEMs.

Exclusions

The new law also specifically defines several exclusions from the consent and content requirements stated above. These exclusions include CEMs sent from registered charities and political parties seeking donations or contributions, between persons with a personal or family relationship, through certain third-party referrals, by certain foreign entities and between organizations with a relationship (if the message concerns the affairs or duties of the organization).

Penalties for Violations

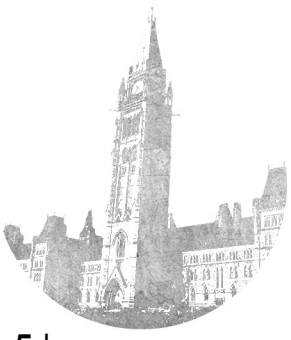
The penalties for noncompliance with CASL are severe. Penalties for sending unsolicited commercial email messages are as follows:

- **Up to $10 million** for corporations **per violation**; or
- **Up to $1 million** for individuals **per violation**.

In 2017, a private right of action will come into force that allows individuals who feel they have been affected by a violation of the law to file a lawsuit in court. This private right of action also opens the door for anti-spam class action lawsuits, with maximum damages capped at **$1 million per day**. Furthermore, under this provision, directors and officers can be held personally liable for violations of the law if they directed, authorized or consented to the violation of the law.

Recommendations for Compliance

There are several steps businesses can take today in order to ease the burden of complying with the law once it goes into effect. Organizations need to ensure that their CEMs meet the form requirements of the CASL. These requirements include obtaining express

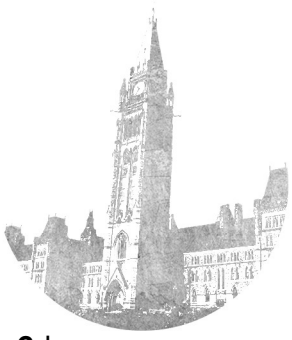


or implied consent and providing the following in each CEM:

- Information identifying the person who sent the message and/or the person on whose behalf it was sent;
- Information enabling the recipient to contact the sender of the message; and
- A mechanism allowing the recipient to unsubscribe to CEMs from the sender.

All organizations should be aware that consent cannot be obtained by sending a request for consent once the law is in effect. When the law comes into force on July 1, 2014, sending an email to obtain consent to send CEMs will be prohibited. However, organizations may obtain consent through electronic means until the law goes into effect.

Contact Excalibur Insurance Group or legal counsel with any questions.



© 2013, 2014 Zywave, Inc. All rights reserved.

CASL-compliant Commercial Electronic Messages

On July 1, 2014, most provisions of Canada's Anti-Spam Legislation (CASL) will come into force. The purpose of this law, in part, is to regulate unsolicited commercial electronic messages (CEMs), commonly referred to as "spam." If your company sends CEMs, you should take note of the law and examine the effect it may have on your business practices. This article outlines steps your company should take prior to July 1 to ensure compliance.

What's Changing?

The law will restrict all forms of CEMs sent via telecommunication, including email messages, text messages, instant messages and messages sent through social media sites. In order to qualify as commercial, CEMs only need to encourage commercial conduct and do not need to have an underlying expectancy of profit.

In order to send a CEM, a company must be able to prove that it has consent from the recipient. As such, it's recommended that companies maintain a list of all contacts, how each contact consented to receive CEMs, the date consent was issued and the date consent expires (if it expires).

There are two types of consent: express and implied:

- **Express consent** is obtained when a recipient "opts in" to receive CEMs. Consent can be oral or written and could take the form of an unedited audio recording, paper form or electronic checkbox on a website. For electronic checkboxes, consent cannot be gained by using an unchecked opt-out box or pre-checked opt-in box. The end-user must opt-in or make a positive action to indicate that he or she provides consent. Express consent never expires, but it can be revoked by the recipient.
- **Implied consent** exists when the sender can establish that the recipient implicitly consented to receiving the CEM. Recipient consent is implied if a pre-existing business relationship already exists between the sender and the recipient. Prior business relationships can be established in situations where the recipient purchased a product, agreed to a contract or made a business inquiry. An existing business relationship expires in six months if a prospect doesn't become a client and in two years if a client doesn't renew.

> According to a 2013 Deloitte survey, only 13 per cent of companies understand CASL requirements and have begun applying them to their business.

Implied consent is also granted in certain non-business relationships, including situations where the recipient provided qualifying donations or volunteer work, or the CEM is provided in a conspicuous publication. Implied consent also exists if the recipient provides the electronic address to which the message is sent and does not indicate that he or she not want communications, and if the message is directly related to the recipient's professional role.

Companies that rely on implied consent when sending CEMs need to keep organized, careful records of contacts and consent dates.

This Legislative Take Action is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice. ©2014 Zywave, Inc. All rights reserved.

There are several **exceptions** to the consent rule, which include CEMs sent with the purpose of:

- Providing a requested quote
- Delivering a product, service or product upgrade
- Providing safety, warranty or recall information about a product the recipient has already purchased
- Completing commercial transactions
- Providing information about an employment relationship

How to Prepare a CEM

- **Establish a CASL compliance committee** by pulling together key voices from senior management, marketing, legal, IT, HR and risk management.
- **Complete a CEM inventory** that includes email addresses for all current contacts (including clients, suppliers, business partners, community relationships, donors and others), a record of how they consented to receiving CEMs, the date of consent and the date consent expires.
- **Solicit express consent from existing contacts** before July 1, 2014. A great way to do this is to establish a monthly email newsletter. Insert a catchy tagline in your email template, such as "We value your privacy. Click here to provide your express consent and continue receiving communication from *company name*" and create a hyperlink to the express consent form on your website.
- **Clean up your data.** A few weeks prior to July 1, 2014, clear your database of contact information for any recipients for whom you cannot prove consent.
- **Create email templates that include required information** such as sender contact information and an opt-out mechanism.
- **Document your efforts** in case you get audited. Along with the CEM inventory, it's also a good idea to implement an internal CASL compliance policy.
- **Educate employees** about when it's legal to send a CEM. Provide training on your CASL compliance policy and corporate procedures.
- **Contact third parties** that would send emails on behalf of your company. Ensure they have CASL compliance policies in place. Additionally, consider incorporating language into your contract that ensures the third party will communicate with you regarding opt-outs in a timely fashion, alert you if it is cited for violation of CASL and indemnify you for any costs or damages arising from its breach of CASL.
- **Cover all of your bases** by consulting with Excalibur Insurance Group about your insurance options. Corporations face penalties of up to $10 million per violation of CASL. A fine like this would put many companies out of business.

Your company can and should continue to harness the power of commercial electronic messages, but it is imperative to be prepared to comply with CASL. Contact Excalibur Insurance Group to learn more about compliance as well as options for insuring your company against potential penalties or litigation.

FAQs on CASL and CEMs

On July 1, 2014, most provisions of Canada's Anti-Spam Legislation (CASL) come into force. This law brings sweeping changes to Internet privacy protocols and, once in force, companies will be forced to update electronic marketing practices as well as customer database records in order to comply.

What is the timeline?

July 1, 2014: Portions of the Act that govern commercial electronic messages (CEMs) come into force.

January 15, 2015: Sections of the Act governing installation of computer programs or software will come into force.

July 1, 2017: The Private Right of Action provisions come into force. The three year transition period for CEMs ends.

Is there a transition period?

Beginning on July 1, 2014, there will be a three-year transitional period during which time consent to send CEMS will be implied for any pre-existing business and non-business relationships. A similar consent window will exist for the installation of updates or computer programs. This consent can be revoked by the recipient at any time.

Who does this impact?

Anyone who makes use of CEMs, produces or installs computer programs or is involved with the alteration of transmission data will be impacted. All organizations in Canada, with very limited exceptions, will be impacted as well as any international organization that sends CEMs, installs programs or transmits data into Canada.

What is a CEM?

CEMs are messages that encourage participation in commercial activity. Even if a commercial message is not sent with an expectation of garnering a profit, it still qualifies as a CEM.

The Canada Radio-television and Telecommunications Commission, the Competition Bureau, and The Office of the Privacy Commissioner will share responsibility for enforcement of CASL.

What do I need to know before sending a CEM?

CASL outlines requirements regarding recipient consent as well as content requirements for CEMs. Generally, senders must be able to prove that the recipient has consented to receive the message and must include sender contact information and an unsubscribe mechanism in the message.

Does this law only apply to CEMs?

No. CASL regulates other electronic threats to commerce, like the installation of computer programs, the alteration of transmission data and the installation of malware. It also prohibits unauthorized collection of electronic addresses and personal information (address harvesting) and false or misleading digital representations.

How do I prepare my company?

Companies should immediately begin reviewing contact databases and electronic marketing practices to prepare for the dates the Act comes into force. Additionally, now is the time to seek

This Legislative Take Action is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice. ©2014 Zywave, Inc. All rights reserved.

express consent from contacts, as sending a CEM to do this after July 1, 2014, will be prohibited.

What if I don't comply?

The financial penalties for noncompliance with CASL are severe. Penalties for sending unsolicited commercial email messages are as follows:

- Up to $10 million for corporations per violation
- Up to $1 million for individuals per violation

Additionally, when the Private Right of Action comes into force in 2017, individuals who feel they have been affected by a violation of the law will be able to file a suit in court. This private right of action also opens the door for anti-spam class action lawsuits, with maximum damages capped at $1 million per day. Furthermore, under this provision, directors and officers can be held personally liable for violations of the law if they directed, authorized or consented to the violation of the law.

CASL: Computer Program Compliance

On Jan. 15, 2015, Section 8 of Canada's Anti-Spam Legislation (CASL) regulating the installation of computer programs will come into force. The purpose of this section of CASL is to prohibit the installation of harmful malware and spyware and to set limits regarding commercial electronic messages (CEMs) that are sent via installed computer programs. If your company installs a computer program and/or your installed product sends CEMs from the computer system on which it is installed, you should take note of the law and examine the effect it may have on your business practices. This article outlines steps your company should take prior to Jan. 15, 2015, to ensure compliance.

CASL and Computer Program Installation

Section 8 of CASL states: "A person must not, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system unless:

a) The person has obtained the express consent of the owner or an authorized user of the computer system and complies with subsection 11(5); or

b) The person is acting in accordance with a court order."

It is important to understand the key terms in this section as CASL defines them:

- **Commercial activity:** Any transaction of commercial character, regardless of whether there is an expectation of profit or not
- **Install:** No definition is provided for this term in the Act. However, installation of a computer program generally occurs when one party sets up a program or service on another party's computer system.

> Only 13 per cent of organizations understand CASL requirements and have begun applying them to their businesses, according to a 2013 Deloitte survey of 100 financial services business leaders.

- **Computer program:** Data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function
- **Computer system:** A device or a group of interconnected or related devices one or more of which (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control functions, and (ii) may perform any other function
- **Express consent** exists when a recipient "opts in" verbally or in writing. Express consent never expires, but it can be revoked by the recipient.

How to Comply

To comply with CASL, the party installing the computer program must:

- Request consent in an approved manner. Purpose for consent, sender contact information and an unsubscribe mechanism must be present. Additionally, the sender must clearly and simply describe the function and purpose of the computer program to be installed.

- If the program performs any of the functions below, the person requesting consent must also clearly, prominently, and separately from the licence agreement, describe the program's material elements, including nature ,purpose, and reasonably foreseeable impact on the operation of the computer system:
    - Collects personal information stored on the user's system
    - Interferes with the user's control of the system
    - Changes the interface or settings of the system without authorization from the user
    - Changes or interferes with data stored in the system
    - Causes the system to communicate with another computer system without user authorization
    - Installs a program that can be activated by a third party without user authorization
- Remove or disable the computer program free of charge and as soon as feasible if consent is revoked. Consent may be revoked if user finds program performs functions for which consent was not provided.

Exemptions

The following are exemptions to the computer program installation requirements under CASL:

- Persons acting on a court order
- Updates or upgrades to computer programs for which consent for installation has already been granted
- Programs necessary to correct a failure that occurred in the computer system or program and is installed only for that purpose.
- Installation of a program that is a cookie, HTML code, JavaScript, operating system or any other program; such installation can only run through the use of another computer program whose installation or use the person has previously expressly consented to.
- Actions by the user that reasonably suggest that the user consents to the program's installation

Penalties

The financial penalties for noncompliance with CASL are severe:

- Up to $10 million for corporations per violation
- Up to $1 million for individuals per violation

Additionally, when the Private Right of Action comes into force in 2017, individuals who feel they have been affected by a violation of the law will be able to file a suit in court. This private right of action also opens the door for anti-spam class action lawsuits, with maximum damages capped at $1 million per day. Furthermore, under this provision, directors and officers can be held personally liable for violations of the law if they directed, authorized or consented to the violation of the law.

Contact Excalibur Insurance Group to learn more about CASL compliance as well as options for insuring your company against potential penalties or litigation.

CEM Inventory

Directions: Use this inventory to house records of all contacts, mechanism of obtaining consent, and expiration of consent (if applicable). Additionally, store information regarding recipients who have opted out of receiving CEMs from your company. Make sure to record information for contacts of all types, not just clients. Include suppliers, business partners, community relationships, donors and more. This table also exists as an Excel Worksheet. Ask Excalibur Insurance Group for a copy.

Name	Email	Express Consent	Implied Consent	Exemption	Consent Obtained	Consent Expires	Consent Mechanism
Sample Person	Sample.person@fakeemail.com		X		8/17/2013	8/17/2015	Existing business relationship – product purchase

FORM

CASL Compliance Agreement

This SAMPLE agreement is of general interest and is not intended to apply to specific circumstances. Make sure to consult legal counsel to customize this agreement prior to implementation.

The following compliance provisions are made on , in order to comply with Canada's Anti-Spam Legislation between

,

and

[Third Party Vendor]
[Address]
[City], [Province] [Postal Code]

RECITALS

WHEREAS, [Third Party Vendor] sends commercial electronic messages, alters transmission data or installs computer programs, software or updates on behalf of

WHEREAS, desires that [Third Party Vendor] provide such services

IN CONSIDERATION of the mutual agreements and covenants contained in this Agreement, and [Third Party Vendor] agree as follows:

AGREEMENT

1.1 Scope of Services

[Third Party Vendor] may distribute CEMs; alter transmission data; or install computer programs, software or updates on behalf of in the following circumstances:

Circumstance 1;

Circumstance 2; and

Circumstance 3.

[Third Party Vendor] and agree to follow the below procedures when a recipient "opts out" or "unsubscribes" to distribution:

Outline procedure for taking care of "opt out" or "unsubscribe" requests

Outline procedure for taking care of "opt out" or "unsubscribe" requests

Outline procedure for taking care of "opt out" or "unsubscribe" requests

[Third Party Vendor] agrees to identify as a referral source for the purpose of the "first CEM after referral" exception.

1.2 Disclosures and Record Keeping

[Third Party Vendor] agrees to maintain a contact list in relation to CASL obligations. List will include:

Contact name;

Virtual address(es);

Type of consent issued (for example, implied consent—requested estimate); and

Date consent expires.

[Third Party Vendor] will maintain a database of express consent records; including but not limited to:

Audio recordings;

Paper forms; and

Records of website checkbox selection.

Records must include:

The manner in which consent was obtained;

A physical record of consent; and

The time/date consent was obtained.

will be notified within two business days of any “unsubscribe” or “opt out” requests.

[Third Party Vendor] will maintain records of CASL compliance and make available such records upon request.

has permission to audit [Third Party Vendor]’s compliance records as deemed necessary and may take copies of records if needed to facilitate the audit process.

[Third Party Vendor] agrees to notify within2 business days if cited by Canada Ratio-television and Telecommunications Commission (CTRC) for violation of CASL.

1.3 Indemnity

will be indemnified for any costs or damages arising from service provider’s breach or alleged breach of CASL.

[Third Party Vendor] agrees to comply with all applicable CASL requirements.

SIGNATURES

I have read, understand and agree to comply with the above clauses. My signature serves as proof that I agree to the tenants of our business partnership with .		
NAME:	**SIGNATURE:**	**DATE:**
NAME:	**SIGNATURE:**	**DATE:**

POLICY

CASL – CEM Compliance Policy

Location:
Effective Date:
Revision Number:

Purpose

One of the main purposes of Canada's Anti-Spam Legislation is to regulate unsolicited commercial electronic messages (CEMs). Non-compliance with CASL will bring heavy penalties. Since we are a company that sends CEMs, the purpose of this policy is to ensure that everyone sending CEMs on behalf of is in compliance with the law and to provide the security framework upon which all CEM delivery efforts will be based. This policy defines appropriate and authorized behaviour for personnel approved to send CEMs on behalf of .

Scope

All electronic messages sent from the network to outside organizations or persons will be presumed to be CEMs and will therefore fall under the guidelines of this policy. This CASL – CEM Compliance Policy applies to all employees, interns, contractors, vendors and other parties sending electronic messages on behalf of .

Definitions

- **Canada's Anti-Spam Legislation (CASL)**: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act.
- **Electronic address**: An address used in connection with the transmission of an electronic message to an electronic mail account, an instant messaging account, a telephone account or any similar account.
- **Electronic message**: A message sent by any means of telecommunication, including a text, sound, voice or image message.
- **Commercial electronic message (CEM)**: CEMs are commercial electronic messages that encourage participation in commercial activity. Even if a commercial message is not sent with an expectation of garnering a profit, it still qualifies as a CEM.
- **Commercial activity**: Any transaction of commercial character, regardless of whether there is an expectation of profit or not. All emails you send from your work email will be treated as commercial.
- **Express consent**: Permission obtained when a recipient "opts in" to receive CEMs. Consent can be oral or written and could be an unedited audio recording, paper form or electronic checkbox on a website. Express consent never expires, but it can be revoked by the recipient. will maintain records of all contacts for whom express consent exists.
- **Unsubscribe**: A withdrawal of consent to receive CEMs
- **Social networking sites:** Specific online communities of users, or any website that links individuals electronically and provides a forum where users can connect and share information. These websites can be general or tailored to specific interests or certain types of users. Examples of popular social networking sites include Facebook®, Twitter®, Google+®, YouTube®, LinkedIn®, Foursquare®, Instagram® and TUMBLR®. The list of domains that constitute social networking sites is always growing and changing due to the nature of the Internet.

Policy Guidelines

All employees, contractors, vendors and any other person sending CEMs on behalf of must adhere to the following policies:

- All information systems within are the property of and will be used in compliance with policy.
- All users will report any irregularities found in incoming or outgoing CEMs and the CEM delivery system to the IT team immediately upon detection.
- The CEM delivery system is subject to monitoring at all times. Use of the CEM delivery system constitutes acceptance of this compliance policy.
- Release of CEMs will be at the discretion of . All requests for release should be submitted to the IT team.
- Users will not use devices to send CEMs without prior approval from management or another designated representative.
- Users will not use devices to conduct personal business.
    - No personal emails should be sent from a email address.
    - No instant messaging should be conducted with parties outside of .
    - Employees are prohibited from using social networking sites to conduct personal or company business.

CEM Recipients

- Employees, interns, contractors, vendors and anyone else sending CEMs on behalf of are to send CEMs ONLY to the electronic address of the parties listed on the Approved CEM Recipients List, which can be found **AT THIS LOCATION**.
- All employees must ONLY use the approved email template in order to gain consent from a party NOT already on the Approved CEM Recipients List. The approved email template can be found **AT THIS LOCATION**.

CEM Components and Guidelines

- All CEMs must contain:
    - contact information, clearly laid out. This includes sender first and last name, sender email address, company name, company mailing address, company telephone number and company Web address.
    - If the CEM is to be sent on behalf of another party at , the name of this party and the sender must both be included, in addition to the information listed above.
    - An “unsubscribe” link, clearly visible.
- Employees are prohibited from modifying the existing signature or contact information.
- Employees are prohibited from removing the “unsubscribe” tool inherent in the approved email templates.
- Employees must follow all approved guidelines on how to craft subject lines and emails messages that are not false or misleading. The approved guidelines can be found **AT THIS LOCATION**,
- All employees must attend the required training session on sending CEMs. Course content will include information on where to access the Approved CEM Recipients List, how to obtain consent if it does not yet exist, and how to craft a compliant CEM subject line and message. Proof of training attendance will be kept on file with HR.

Unsubscribe Requests

- All “unsubscribe” requests must be immediately forwarded to the **LIST APPROPRIATE PARTY** at **LIST APPROPRIATE EMAIL ADDRESS** in order to ensure prompt processing of the request and to maintain accurate records. EMPLOYEES MUST NOT SEND ANY FURTHER COMMUNICATION TO THE UNSUBSCRIBED PARTY.

CASL – CEM Compliance Policy

Commercial electronic messages (CEMs), and the tools that create, store and distribute them, are vital to the long-term health of our organization. It is for this reason we have established the CASL – CEM Compliance Policy.

Compliance with CASL is of utmost importance, and all employees are expected to understand and actively participate in maintenance of corporate compliance. encourages its employees to take a proactive approach in identifying potential problems or violations of CEM delivery by promptly reporting issues to the IT team immediately.

Prior to using equipment, each employee is expected to have read the entire CASL – CEM Compliance Policy, which includes:

- Purpose
- Scope
- Definitions
- Policy Guidelines
- CEM Recipients
- CEM Components and Guidelines
- Unsubscribe Requests

Each employee is also expected to attend the CEM Compliance training sponsored by .

If you have any uncertainty regarding the content of this policy, you are required to consult your supervisor. This should be done prior to signing and agreeing to the CASL – CEM Compliance Policy.

- I have read and understand the CASL – CEM Compliance Policy, and I understand the requirements and expectations of me as an employee.

- I have attended the sponsored training and understand my responsibilities when crafting and sending a CEM on behalf of the company.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

CEM Training Completion Date: _____

Spam, Phishing and Spyware Defined

Companies nationwide are now storing much of their information on computer servers and databases, and because that information has great value, hackers are constantly looking for ways to steal or destroy it. In fact, according to the 2013 Norton Report, over 7 million people were victims of cyber crime last year, and it cost Canadians $3 billion—roughly $380 per victim.

A computer intrusion could cripple your company, costing you thousands or millions of dollars in lost sales and/or damages. Hackers can obtain access to personal information in many ways, including spam, phishing and spyware. Below are definitions and examples of these three types of scams.

Spam

Spam is any unsolicited electronic content, often known as junk mail. It can take the form of a text message, direct mailer, phone call or email message. Spam emailing in particular is quite common, and spam emails often contain some form of scam, virus and/or invasive or inappropriate content.

Prevent your company from falling victim to scams and viruses in spam messages by teaching employees to ask the following questions while using company email:

- *Do you know the sender?* Beginning July 1, 2014, all senders are required to identify themselves when sending a commercial electronic message. If employees don't recognize the sender's name, they should not open the email.
- *Is the grammar and spelling poor?* Sometimes spammers intentionally misspell words or use words incorrectly to sneak emails past your company's spam filter. Encourage employees to be on the lookout for this trick.
- *Have you received something from this sender before, but now the email looks drastically different?* It could be a fraudster. Encourage employees to look at all emails with a discerning eye, even those coming from known senders.
- *Does it sound too good to be true?* If it sounds too good to be true, it probably is.
- *Is it in your spam folder?* Make sure employees know the danger of opening messages that go straight to their spam folder. Many people consider spam to be annoying but harmless. However, the majority of computer viruses are "caught" via email. Employees should never open messages that your system has designated as spam.

Additionally, company policies regarding computer use are an effective way to reduce the impact that spam has on your system. Minimally, your policy should require employees to:

- Turn off computers before leaving the office each day. Spam and viruses can strike a computer at any time when it is sitting idle and still connected to the Internet.
- Keep work email communications separate from personal communications. Employees should use a personal email that is not connected to the company email for personal communications.
- Limit the amount of time employees can spend on social media sites (for example, only allow them to use the sites during breaks), or prohibit their access entirely during the workday.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2013-2014 Zywave, Inc. All rights reserved.

Phishing
A phishing scam is a phony email or pop-up message used to lure unsuspecting Internet users into divulging personal information, such as credit card numbers and account passwords, that will later be used by hackers for identity theft. A phisher's email can be very persuasive and believable if he or she is impersonating a well-known organization or individual.

Keep employees safe from phishing scams by teaching them to:

- Be extremely wary of urgent email requests for any personal or financial information (their information or a client's).
- Call the company or individual in question with the number listed on the corporate website or in the phone book. Avoid using phone numbers within the email, as they could be phony too.
- Do not use the links included in the email unless you are certain that the email is legitimate.
- Do not divulge personal or financial information via the Internet unless the site is secure (sites that start with "https").
- Never disable anti-virus software.

Spyware
Spyware is software that can be installed on a computer without the user's permission, usually as a result of the user opening an attachment and/or downloading an infected file from an untrusted source. Spyware can be used by hackers to "spy" on Internet users, track browsing habits and collect personal information such as credit card numbers.

Signs that spyware may be installed on a computer:

- The computer starts to suddenly run slower.
- Pop-ups appear when the user is offline.
- Internet browser settings are modified. New shortcuts, icons or tool bars may appear.

As most spyware is installed when users download free files from the Internet, it's important to ensure that your employee Internet usage policy has a clause banning employees from opening or downloading personal files on work machines.

Many Internet Service Providers (ISPs) will offer security software to businesses at no charge, so be sure to ask. It is important to be vigilant and cautious about the content your employees open while using the Internet. Risky employee Internet use can have serious consequences for your company. For more information about safe Internet use and developing an employee Internet use policy, contact Excalibur Insurance Group today.

PLAYING IT

SAFE

Be safe and healthy on the job at with these helpful tips provided by Excalibur Insurance Group

Surf the Internet Safely

Helpful tips for staying safe while surfing the Internet

By their nature, computers, tablets, mobile phones and other personal devices are vulnerable machines. Access to the Internet connects these systems and their users to increased information, as well as increased risks. Each day, new threats emerge. Surfing on the Internet is what makes you and your information most vulnerable, so how do you keep yourself safe?

Before You Surf
Always make sure your computer and electronic devices are up to date with the most recent anti-spam, anti-virus and firewall protection that is offered. If you continue to use an outdated version, it might not be strong enough to stop newly created viruses and cyber attacks.

Never purchase your security software through a pop-up ad or suspicious email—these are typically phony advertisements. Instead, research to find a reputable company or get references from friends or co-workers.

Finally, make sure your firewall protection is turned on at all times. An active firewall monitors incoming and outgoing traffic on your device, which is necessary because it protects your computer from hackers trying to gain access and stops your personal information from being sent off into the vast unknown where others may be able to see it.

While You Surf
Wherever you may be—at home, at work or in a public place—there are a few general safety tips to keep in mind while using the Internet:

- Have a primary email address for important matters (like your work email) and a secondary email address that you can give out to family members, or to use for making online purchases.
- If you receive a suspicious email that includes links to a website, don't click on those links. They may appear to direct you to real companies' websites, like your credit card company, but they actually direct you to an entirely different, completely unsafe website.
- Never open an attachment you receive from a questionable email until you've verified that the individual or organization that sent it can be trusted.
- Make sure all of your passwords include letters, numbers and symbols, if possible.
- Use caution when downloading files from the Internet. Make sure you trust the website you're downloading the file from.

Surfing on Public Wi-Fi
When connecting to a Wi-Fi network at a public place like a coffee shop or a restaurant, there are things you need to do to protect yourself from some virtual risks:

Stay Alert for Fraud
Never bypass a website's security policies, even with a familiar company or a routine transaction. Cyber attacks can occur at any time, and often happen when users least expect them.

PLAYING IT SAFE

- Double-check that you are connected to the correct network. Sometimes cyber thieves will make duplicate Wi-Fi hotspots with names very similar to the real one in the hope that unsuspecting users will accidentally connect to the phony hotspot.
- If a certain website asks you whether you want to use encryption while browsing that site, always do so by enabling the Secure Sockets Layer (SSL), or HTTPS setting. These choices can be found most often under the “privacy” section of the website.
- Always choose to surf the HTTPS option of a website over the HTTP one—remember that the S in HTTPS means it’s more secure. If you notice the S has disappeared after you’ve signed in to a site, immediately sign out.
- When using public Wi-Fi, do not go on personal banking websites, and avoid shopping online. It is much easier for thieves to steal the personal information you are putting in to websites when they are logged on to the same network as you.
- Only use your secondary email when you are using public Wi-Fi. This makes it harder for hackers to reach the personal information you may have stored in your primary or work email account.

Use Common Sense

If you ever suspect that a website or link is not legitimate, do not click on it or visit the site! Your device and your identity are at stake. If you are using your device at work, you are also putting your company in jeopardy because hackers that gain access to your device may be able to use the Internet connection to obtain all types of personal information from co-workers, upper management and even your customers or clients.

Change it up

When it comes to passwords, diversification is important. Using the same password on more than one site provides a hacker with easy access to your personal data.

Compliant marketing under Canada's Anti-Spam Legislation

Can I send it?

Is it a commercial electronic message?
(electronic message such as an email, text, image or social media post sent in connection to commercial activity)*

No → **Do not send!**

Yes →

Is the recipient a friend or family member?

Yes → **Send it!**

No →

Are you or the recipient located in Canada?

No → **Do not send!**

Yes →

Do you have express consent?
(oral or written opt-in from recipient)

Yes → **Send it!**

No →

Do you have implied consent?

- Existing business relationship
- Existing non-business relationship**
- Recipient voluntarily discloses or conspicuously publishes electronic contact information and doesn't indicate they don't want communications

Implied consent expires in six months if a prospect doesn't become a client or two years if existing client does not renew relationship

Yes → **Send it!**

No →

Is there an exception? Are you emailing to:

- Provide a quote requested by recipient?
- Confirm an existing commercial transaction?
- Provide warranty, recall or safety information for a product recipient has purchased?
- Inform recipient about employment relationship or benefit plan?
- Deliver a product, product upgrade or service?
- Provide factual information about an existing purchase, subscription, loan or account?

Yes → **Send it!**

No → **Do not send!**

Send it!
Include your contact information and an unsubscribe mechanism.

*For a list of excluded messages, see Section 3 of the Electronic Commerce Protection Regulations

**An existing non-business relationship exists when a recipient donates to or volunteers with a registered charity or public organization OR is a member of the organization's club, association or not-for-profit volunteer association.

The information contained in this document is not intended to be used as legal advice. The reader should consult legal counsel regarding specific legal issues. © 2014 Zywave Inc. All Rights Reserved.

Surf Safe:

Tricks to Recognize Spam Emails

Uses Scare Tactics

- Threatens to delete your account
- Sets an unreasonable timeline – *you must reply by tomorrow*

Asks for Too Much Information

- No reputable company will ask for your Social Insurance number, birth date, bank account number, or credit card number in an email.

Asks for Money

- Especially money that can't be tracked, like cash or a cashier's cheque

Makes an Offer You Can't Resist

- *"You've won our 1,000,000 sweepstakes!"*

Feels a Little Off

- Doesn't refer to you by name
- Typos in the text
- Sender address is unfamiliar or has unusual mix of numbers and words

Symantec Study Shows:

64% of emails sent each day around the world are spam.

© 2014 Zywave Inc. All Rights Reserved.